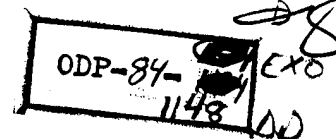


~~CONFIDENTIAL~~

ORD-0832-84

18 July 1984

MEMORANDUM FOR: Distribution

FROM :

Guard System Development Program Manager
Information Systems Research Division
Processing and Analysis Technology Group
Office of Research and Development

SUBJECT : RECON/Guard Program Status Report--13 July 1984
(Evaluation Phase Completion/Confidence Testing Results)

REFERENCE : 1. Guard System Final Report: Sytek TR-84010;
dtd 14 June 1984 (Attachment E)
2. Sytek Letter #TAB-064-84; dtd 12 July 1984
(Attachment F)

I. Purpose:

The purpose of this memorandum is to convey the results of the RECON/Guard Program evaluation phase. The evaluation phase testing of the RECON/Guard prototype system was successfully concluded on 12 June 1984. The RECON/Guard prototype system functioned as required under all security tests. A description of the tests performed is attached (Attachment A).

II. Evaluation Phase Results:

The primary objective of the RECON/Guard prototype evaluation phase was security confidence testing of the prototype system to prove or disprove the validity of the secure architectural principles on which the Guard System is built. The secondary objective was the determination of desired performance features the Guard System should possess in an operational environment. The security evaluation was conducted by OS/ISSG. A draft copy of their report is attached (Attachment B). The operational evaluation was conducted by OCR/IAB. The official OCR report is also in preparation. Both reports will be available for distribution. The findings of the security evaluation were the Guard System is secure and performs its security/control function as required. Thus the secure architectural/design concepts employed in the Guard System have been proven in the most rigorous environment possible.

This document is downgraded
to UNCLASSIFIED upon removal
of Attachment B

~~CONFIDENTIAL~~

SUBJECT: RECON/Guard Program Status Report--13 July 1984
(Evaluation Phase Completion/Confidence Testing Results)

III. Evaluation Phase Test Environment:

The test environment consisted of the Guard Test System (GTS), a RECON test database (2000 records), and two trapdoor programs (one for the GTS and one for the RECON test database access system). Thus the Evaluation Phase Confidence Testing was conducted in the most rigorous and hostile environment realizable.

A. RECON Test Database

The RECON Test Database was comprised of unclassified RECON records restructured to emulate RECON records of all types and classifications. Also the header information of these records was changed slightly as an additional barrier to accidental access to operational RECON data.

B. RECON Trapdoor Program

25X1 The RECON Trapdoor Program was generated by the OCR test team, headed by [] (whose efforts were instrumental in the successful conclusion of the RECON/Guard development and evaluation). The purpose of this trapdoor program was to enable unauthorized manipulation of the RECON test system database in an attempt to defeat the Guard System security features. The trapdoor program operated at the most privileged system level and thus had full access to the RECON test database. The details of this trapdoor program are given in Attachment A.

C. Guard Test System (GTS)

Details of the GTS are given in Attachment C. The GTS is a local area network and a COINS-HAS (Community Online Intelligence Network System-Host Access System) emulation module and a RECON emulation module. Thus the GTS could emulate the COINS-HAS and/or the RECON Test System for evaluation of the RECON/Guard prototype. The GTS also included a trapdoor program which permitted error injection during HAS emulation and/or RECON Test System emulation. This level of testing would not have been possible using an actual HAS or operational RECON.

IV. Summary of Evaluation Phase Testing:

The GTS was constructed to provide a test platform for the RECON/Guard prototype system in the event the RECON Test System

SUBJECT: RECON/Guard Program Status Report--13 July 1984
(Evaluation Phase Completion/Confidence Testing Results)

database and/or the COINS-HAS was unavailable for use in testing the Guard. The GTS was also designed to provide maximum operator access to the information flow within the GTS and between the GTS and the Guard prototype. Thus, via the GTS mechanism, multitudes of errors and error combinations were injected in the Guard processing stream. This would not have been possible without the GTS. Therefore the maximum level of rigor and hostility for the test environment was realized for the Guard prototype security testing and operational evaluation.

Since the COINS-HAS was not available for the Evaluation Phase Confidence Testing, the GTS was used primarily in the COINS-HAS emulation mode. If the COINS-HAS had been available, GTS testing in the HAS emulation mode would still have been necessary, due to the increased rigor achievable only with the GTS. The realization of the GTS permitted the RECON/Guard prototype Evaluation Phase (Confidence Testing) to be completed successfully and within schedule. Additional details are discussed in Reference 1 (Attachment E).

V. Current/Future Efforts:

Current contractor efforts will focus on RECON/Guard Program final report preparation, software verification briefings, and preparation (restructuring) of the prototype RECON/Guard System to serve as the software development platform for the operational Guard System development effort (FY85). This is discussed in Reference 2 (Attachment F).

FY85 efforts will focus on the development of an operational Guard System (Trusted Domain Machine) which will be based on the architectural principles proven in the prototype evaluation. The TDM development will be directed against several applications, primarily CIRS (with COINS interface), interactive RECON, and the FBIS requirement. The Sytek TDM design team will meet with the Agency design team for the above applications for briefings on the detailed functional specification of each proposed application. An example of another possible application for a TDM-type system is given in Attachment D.

VI. Acknowledgements/Recommendations:

The efforts of all Agency components and personnel who contributed to the success of this project is cheerfully acknowledged.

CONFIDENTIAL

SUBJECT: RECON/Guard Program Status Report--13 July 1984
(Evaluation Phase Completion/Confidence Testing Results)

Special appreciation is due the COINS-PMO for attempting to provide a COINS-HAS for the Evaluation Phase testing. Since the need for the HAS equipment was eliminated, by the GTS, and because COINS is an invaluable Community resource, I recommend that the HAS equipment allocated for the RECON/Guard Program be returned to the control of the COINS-PMO for deployment on the COINS network.

I look forward to working with the COINS-PMO and the CIRS design team in defining the TDM interfaces to the projected new COINS-HAS equipment set during the FY85 effort.

25X1

Attachments:

- A. RECON/Guard Confidence Tests
- B. OS/ISSG Draft Evaluation Report
- C. GTS Configuration Diagrams
- D. Additional Application for TDM
- E. Guard System Final Report
Sytek TR-84010 dtd 6/14/84
- F. Sytek Current Status Report
Letter TAB-064-84 dtd 7/12/84

Distribution:

- 1 - D/ORD
- ✓ 1 - D/ODP
- 1 - D/OCR
- 1 - DD/ORD
- 1 - C/PATG
- 1 - C/ISRD
- 1 - RECON Committee Members
- 1 - Contract File

CONFIDENTIAL